Internet Governance (hoofdstuk 1)

Schermer, B.W.; Lodder, A.R.

published in
Recht en Computer (6e druk)
2014

Internet governance

Bart W. Schermer & Arno R. Lodder

1 Inleiding

Het internet bestaat al meer dan veertig jaar, maar kon aanvankelijk alleen worden gebruikt door overheden en wetenschappers. In 1993 werd het internet opengesteld voor het algemene publiek en is vervolgens uitgegroeid tot een integraal onderdeel van onze maatschappij en ons dagelijks leven. Naarmate het belang van het internet toenam, werd ook de vraag hoe wij het internet moeten besturen en reguleren steeds relevanter. Deze vraag is uitermate gecompliceerd: als iedereen waar ook ter wereld informatie beschikbaar kan stellen aan en ontvangen van de hele wereldbevolking, welk recht is dan van toepassing? Wie kan op deze informatie invloed uitoefenen? In dit inleidende hoofdstuk zullen wij de belangrijkste technische kenmerken van het internet bespreken en ingaan op de mogelijkheden en complexiteit van het besturen en reguleren van het internet ('internet governance'). Hiermee vormt dit hoofdstuk ook een basis voor de diverse onderwerpen die in de volgende hoofdstukken aan de orde komen.

2 Wat is het internet?

Voor een goed begrip van het bestuur en de regulering van het internet is het allereerst noodzakelijk om te weten wat het internet is en hoe het werkt.

2.1 Netwerk van netwerken

Het internet is een losjes georganiseerd, wereldomspannend publiek netwerk van autonome computernetwerken [1] De verschillende netwerken zijn fysiek met elkaar verbonden door uiteenlopende elektronische en optische netwerktechnologieën. De apparaten die met het internet verbonden zijn (de knooppunten ofwel 'nodes' op het netwerk) kunnen communiceren met elkaar, omdat zij vrijwillig gebruik maken van dezelfde gestandaardiseerde communicatieprotocollen. De kern van deze protocollen wordt gevormd door de *Internet Protocol Suite*.

De Internet Protocol Suite is ontwikkeld in de jaren zeventig van de vorige eeuw binnen de Defense Advanced Research Agency (DARPA) van het Amerikaanse leger. Het doel van DARPA was om een robuust, gedistribueerd communicatienetwerk te ontwikkelen. Binnen een gedistribueerd netwerk zijn er geen centrale punten waar het hele netwerk van afhankelijk is. Wanneer een node uit het netwerk wegvalt (bijvoorbeeld door een kernaanval op een stad), kan binnen een gedistribueerd netwerk de communicatie via een andere route omgeleid worden. Op deze manier zou de communicatie van het Amerikaanse leger nooit platgelegd kunnen worden door aanvallen op de centrale punten in het netwerk (zogenaamde single points of failure). Onderstaande figuur van Paul

[1] Zie Request for Comments 1602 via: http://www.ietf.org/rfc/rfc1602.txt.

Baran, de grondlegger van het internet als gedistribueerd netwerk, laat verschillende netwerk configuraties zien.[2]

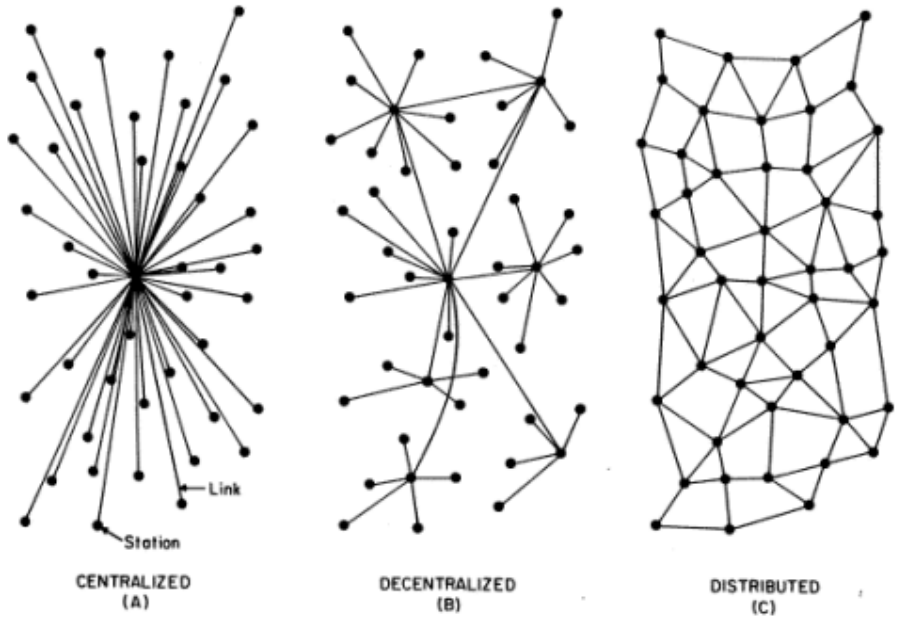


FIG. 1 — Centralized, Decentralized and Distributed Networks

Om het verkeer om te leiden via een andere route werd gebruik gemaakt van *packet switching* in plaats van het toen gangbare *circuit switching*. Bij circuit switched-communicatie wordt er een specifiek communicatiecircuit opgesteld dat de communicatie moet volgen. Als dit circuit onderbroken wordt, dan kan de communicatie niet plaatsvinden. In packet switched-netwerken wordt de communicatie opgedeeld in kleine pakketjes die vervolgens de meest efficiënte route door het netwerk zoeken naar de eindbestemming. Wanneer een verbinding tussen twee netwerknodes geblokkeerd is, dan kunnen de pakketjes om deze blokkade heen routeren. Bij de ontvanger worden de losse pakketjes vervolgens weer samengevoegd tot het oorspronkelijke bericht. De Internet Protocol Suite werd de standaard voor deze packet switched-communicatie.

Na de adoptie van de Internet Protocol Suite door het Amerikaanse leger volgden ook de academische wereld en de private sector. Inmiddels is de Internet Protocol Suite de communicatiestandaard waar het internet op draait.

2.2 TCP/IP

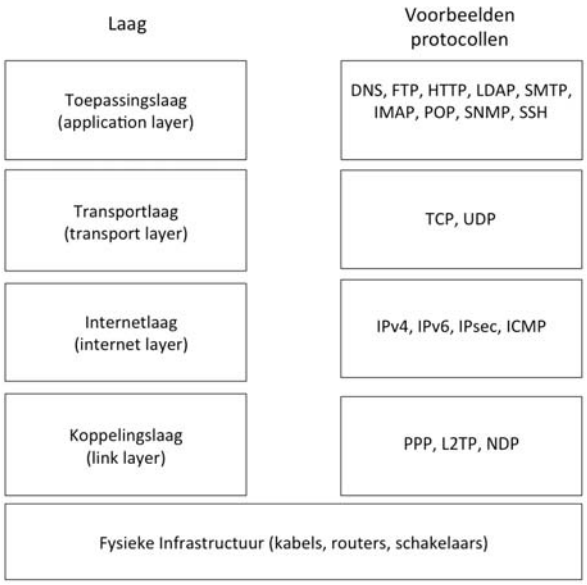
Het Transmission Control Protocol (TCP) en het Internet Protocol (IP) zijn de belangrijkste en bekendste protocollen die deel uitmaken van de Internet Protocol Suite. Gezamenlijk verzorgen deze twee protocollen de packet switched-communicatie op het internet. Elke node die verbonden is met het internet heeft een eigen IP-adres. Aan de hand van het IP-adres weten routers, dat wil zeggen de apparaten die het internetverkeer regelen, welke pakketjes met informatie naar welke computer gestuurd moeten worden. TCP werkt ‘bovenop’ het IP. TCP geeft de garantie dat de pakketjes met gegevens aankomen zoals ze verstuurd werden en vangt eventuele fouten in de gegevens of in de

[2] Zie: Baran, P. (1964), Rand Memoranda on Distributed Communication (3240-PR, hoofdstuk 1), via: http://www.ibiblio.org/pioneers/baran.html.

volgorde van de gegevens op. Als een pakketje aankomt, wordt er via TCP een bevestiging (acknowledge) verstuurd. Als er bij de zender van het pakketje na een bepaalde wachttijd nog geen bevestiging binnen is, wordt het pakketje opnieuw verstuurd.

2.3 Internet: een gelaagde infrastructuur

Conceptueel kunnen wij het internet voorstellen als een gelaagde infrastructuur.[3] Iedere laag in het model vervult een specifieke rol in de communicatie (met behulp van eigen, specifieke protocollen) en maakt het mogelijk voor de bovenliggende laag om te werken.



De bovenste laag wordt de toepassingslaag (application layer) genoemd. In deze laag hebben de digitale gegevens de vorm van (voor de mens) begrijpelijke informatie, zoals tekst en getallen. De applicatielaag wordt gebruikt door netwerkprogramma's, zoals browsers of e-mailprogramma's. De onderste laag is de fysieke laag en beschrijft de elektrische en mechanische kenmerken van het netwerk, van de specificaties van het elektrische signaal tot de kabeltypes, de stekkers en de spanning op de kabels. Bij verzending gaat data van de bovenste naar de onderste laag, waarbij telkens nieuwe gegevens toegevoegd worden ten behoeve van de route over de infrastructuur, de volgorde van de gegevens en de foutcorrectie.

2.4 De verbinding van netwerken: interconnectie

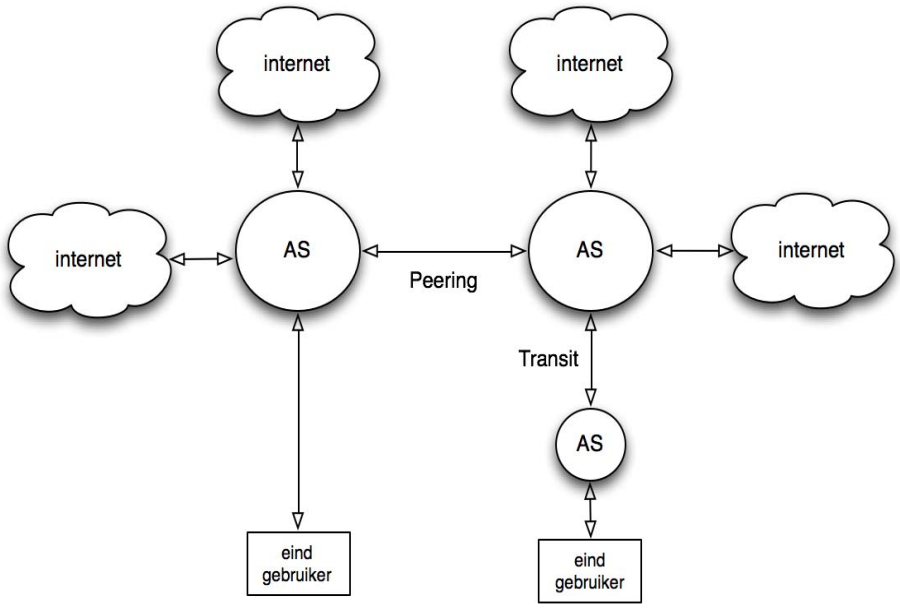
In de context van het internet worden IP-netwerken (of netwerken van netwerken) die zelfstandig functioneren en beheerd worden Autonome Systemen (AS) genoemd. Binnen een autonoom systeem zijn afspraken gemaakt over de routering van verkeer tussen de nodes binnen het eigen netwerk. Alle nodes binnen het eigen netwerk (of de netwerken) kunnen met elkaar communiceren, maar niet met nodes buiten het autonoom systeem en de rest van het internet.

Om elkaars gebruikers, alsmede andere netwerken (de rest van het internet) te bereiken, kunnen eigenaren van autonome systemen afspraken maken over het uitwisselen van gegevens tussen hun

[3] Er zijn diverse 'lagen modellen' van het Internet ontwikkeld. Wij hanteren het vierlaags TCP/IP model zoals omschreven in RFC1122. Wij hebben hier de fysieke laag aan toegevoegd.

netwerken (interconnectie). Deze interconnectie-afspraken bestaan in twee vormen: 1) *peering* en 2) *transit*. Bij peering vindt de uitwisseling van verkeer met gesloten beurs plaats, bij transit biedt het ene AS aan het andere AS (meestal een kleinere provider) toegang tot de rest van het internet tegen een vergoeding (*transit fee*).

Om verkeer te routeren tussen verschillende netwerken op het internet, wordt gebruik gemaakt van het *Border Gateway Protocol* (BGP).[4] Ieder autonoom systeem krijgt een eigen AS-nummer toegewezen waardoor het herkenbaar is binnen het grotere netwerk. Wanneer twee autonome systemen met elkaar contact maken via het BGP, kunnen alle nodes binnen de twee autonome systemen met elkaar in contact komen.



Wanneer meerdere autonome systemen afspraken maken omtrent peering (het koppelen van hun netwerken) ontstaat een internetknooppunt. Deze knooppunten worden ook wel *Internet Exchanges* (IX) genoemd. Amsterdam heeft één van de grootste Internet Exchanges ter wereld: de Amsterdam Internet Exchange (AMS-IX).

2.5 Het wereldwijde web

De meeste mensen denken bij het internet aan surfen op het World Wide Web. Het is echter van belang het web als internettoepassing te onderscheiden van het internet als communicatie-infrastructuur. Weliswaar is het web één van de belangrijkste internettoepassingen, maar het is niet synoniem met het internet. Gegeven het belang van deze dienst voor de ontwikkeling en het gebruik van het Internet dient er vanuit reguleringsperspectief wel apart aandacht aan te worden besteed.

[4] Zie RFC 4271 (via: http://www.ietf.org/rfc/rfc4271.txt) en RFC 6286 (http://tools.ietf.org/html/rfc6286).

Het wereldwijde web wordt mogelijk gemaakt door het *Hypertext Transfer Protocol* (HTTP). Dit is het protocol voor de communicatie tussen de *webclient* (zoals een *browser*) en een *webserver* (de plaats waar bijvoorbeeld websites zijn opgeslagen). Door middel van HTTP doet de client een verzoek aan de server. Elk verzoek bevat een zogenaamde *Uniform Resource Locator* (URL) die naar specifieke data op de webserver verwijst (bijvoorbeeld de locatie van een webpagina, afbeelding of emailadres).

URL's dienen als hyperlinks waarmee gebruikers naar verschillende pagina's binnen een website, naar externe websites of naar documenten doorgestuurd kunnen worden.

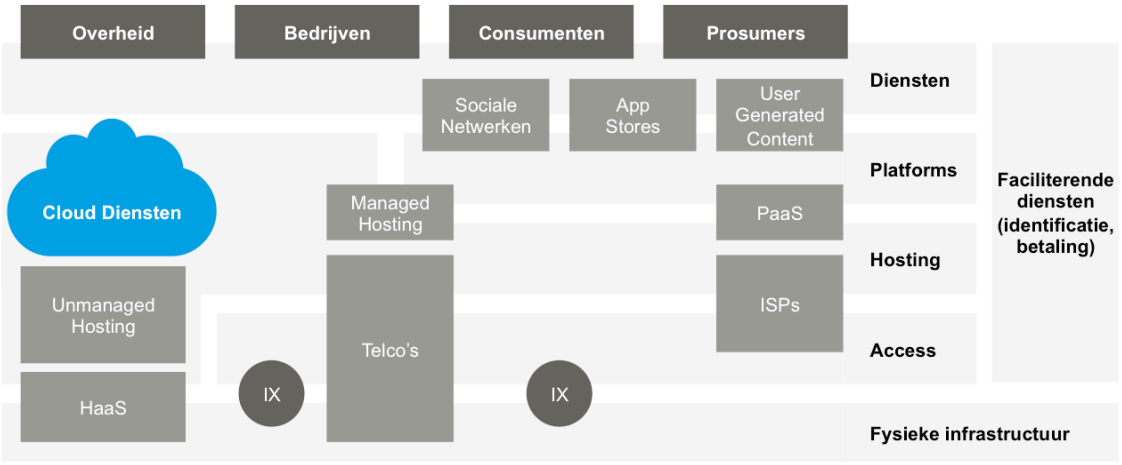
2.6 Domeinnamen en het DNS

Het *Domain Name System* (DNS) is het netwerkprotocol dat op internet gebruikt wordt om domeinnamen te koppelen aan IP-adressen. Een IP-adres is een reeks getallen die een apparaat op het internet identificeert. Het DNS is ontwikkeld omdat het voor mensen te ingewikkeld is om IP-adressen te onthouden. Wanneer een gebruiker een domeinnaam intypt in zijn browser (bijvoorbeeld www.rechtspraak.nl), dan wordt via het DNS opgezocht naar welk IP-adres deze domeinnaam verwijst (in dit geval 159.46.193.17).

Domeinnamen bestaan uit een zelf gekozen naam en een specifieke extensie, zoals .com, .net, .edu, .nl of .es. Gebruikers kunnen zelf een domeinnaam kiezen en deze laten registreren bij een zogenaamde *registry*, wanneer de naam niet al door iemand anders is geclaimd. Domeinnamen als .com, .net en .edu worden *Top Level Domains* genoemd (TLDs), domeinnamen die een specifiek land aanduiden (.nl voor Nederland en .es voor Spanje bijvoorbeeld) worden Country Code Top Level Domains genoemd (ccTLDs). In 2012 zijn generieke top level domeinen (gTLDs) geïntroduceerd waarbij het mogelijk is om zelf een extensie te creëren (zoals .book, .hotel of .app).

2.7 Belangrijke internetdiensten

Naast een gelaagde structuur in de communicatie is er ook een lagenstructuur in het aanbieden van internetgerelateerde diensten. Op diverse niveaus zijn actoren actief om het internet te beheren en te faciliteren. In het onderstaande schema is grofweg aangegeven welke typen diensten er kunnen worden onderscheiden.



In het kader van internet governance zijn de volgende diensten specifiek van belang.

2.7.1 Toegang tot het internet (access)

Een internet *access provider* biedt particulieren en bedrijven de faciliteiten om via een vaste computer of een mobiel apparaat verbinding met het internet te maken. Een access provider slaat in principe geen informatie op, maar functioneert primair als doorgeefluik voor internetverkeer (*mere conduit*). De access provider kan informatie wel tijdelijk opslaan (*caching*) om snellere toegang tot de data mogelijk te maken.

2.7.2 Hosting

Een internet *hosting provider* levert diensten voor het opslaan en beschikbaar maken van gegevens, zoals een website. Bij hosting kunnen tal van vormen worden onderscheiden. Allereerst is er het onderscheid tussen *managed hosting* en *unmanaged hostin*g. In het eerste geval worden de servers beheerd door de hoster, in het tweede geval is de klant zelf verantwoordelijk voor het beheer van de aangeboden server (onderhoud, service, et cetera). Een tweede onderscheid is dat tussen *dedicated hosting* en *virtual hosting*. In het eerste geval heeft een gebruiker een eigen, specifieke server (met een eigen IP-adres), in het tweede geval deelt de gebruiker de fysieke server met andere gebruikers en heeft slechts een eigen afgesloten deel van de server ter beschikking.

2.7.3 Platformdiensten

Tot eind jaren negentig was het dominante dienstverleningsmodel op internet relatief statisch. Diensten die werden aangeboden aan de gebruiker waren primair statische internetpagina's met informatie. Rond de eeuwwisseling kwam hier verandering in met de komst van diensten die individuele gebruikers (zowel bedrijven als consumenten) in staat stelden om zelf ook informatie te produceren en via het internet te distribueren. Door platformdiensten zoals sociale netwerken (Myspace, Hyves, Facebook, LinkedIn), (micro)blogging diensten (Wordpress, Twitter en Tumblr), videosites (YouTube, Vimeo) en fotosites (Flickr, Instagram) zijn gebruikers inmiddels ook actieve participanten op het internet. Naast deze zogenaamde sociale media of 'Web 2.0' toepassingen zijn er ook andere platformdiensten, zoals veilingsites (Marktplaats, eBay) en opslagdiensten (Mega, Rapidshare, WeTransfer).[5]

2.7.4 De 'Cloud'

Een belangrijke ontwikkeling in de manier waarop internetdiensten worden aangeboden, is cloud computing. Door middel van cloud computing kunnen hardware, applicaties en gegevens via het internet ter beschikking worden gesteld aan de eindgebruiker. In feite zijn clouddiensten specifieke vormen van platform- en hostingdiensten, waarbij de dienst op afstand wordt geleverd. Bekende voorbeelden van clouddiensten zijn email (Gmail, Hotmail), kantoorsoftware (Office 365, Google Docs, Salesforce) en opslag (Skydrive, Amazon Clouddrive, iCloud).

2.8 De verdere ontwikkeling van het internet

Bovenstaand zijn de belangrijkste technische kenmerken van het internet beschreven, maar het internet en ook de diensten die van het internet gebruik maken ontwikkelen zich razendsnel. In dat kader staan wij daarom in deze paragraaf kort stil bij enkele toekomstige ontwikkelingen op het gebied van het internet.

---

[5] Zie ook A.R. Lodder e.a. (2010). Recht en web 2.0. (NVvIR publicatiereeks, 27). Amsterdam: Lulu.

Door de ontwikkeling van draadloze netwerktechnologieën en miniaturisering van computertechnologie kunnen steeds meer apparaten en objecten worden uitgerust met internettoegang. Een volgende logische stap in deze ontwikkeling is het koppelen van fysieke voorwerpen aan het internet: *the Internet of Things*. Deze ontwikkeling is al geruime tijd bezig in een industriële context, waarbij via het internet fysieke apparaten (waterpompen, kleppen) via zogenaamde SCADA- en PLC-systemen worden aangestuurd.[6] Maar ook in de fysieke wereld worden steeds meer objecten uitgevoerd met netwerk en computertechnologie, denk bijvoorbeeld aan de draadloze OV-chipkaart, de slimme energiemeter en intelligente auto's.

In het verlengde van het Internet of Things ligt de visie van *Ubiquitous Computing* en *Ambient Intelligence*, waarin de mens wordt omringd door een onzichtbaar netwerk van intelligente computers, sensoren en andere ICT-middelen. In deze visie staat de gebruiker centraal: de intelligente, onzichtbare ICT-infrastructuur is zich 'bewust' van de personen in de omgeving en kan anticiperen en reageren al naar gelang de wensen en de behoeften van deze personen. Deze ontwikkeling tekent zich inmiddels duidelijk af met de toepassing van *Radio Frequency Identification* (RFID), intelligente camera's en sensornetwerken.[7]

Tegelijkertijd is er een ontwikkeling gaande die bekend staat onder de naam *Augmented Reality*, waarbij (via het internet verkregen) informatie direct zichtbaar is in onze fysieke wereld. In dit concept wordt via een scherm (in een mobieltje of bril) een informatielaag over de fysieke werkelijkheid heen geprojecteerd. Hiermee wordt het mogelijk om in real time digitale informatie te krijgen over mensen en objecten in de fysieke wereld. Google Glass en Layar zijn voorbeelden van praktische toepassingen van Augmented Reality.

3 Wat is internet governance?

Het beheer van en de controle over het internet wordt gevat onder de noemer *internet governanc*e. Governance kan breed worden gedefinieerd als:

"Het proces van interactie en besluitvorming door actoren betrokken in een collectief vraagstuk, dat leidt tot de creatie of bevestiging van sociale normen en instituties."[8]

Anders dan bij fysieke wegen waar in de wet is aangegeven wie de wegbeheerder is,[9] zijn er bij het internet vele beheerders op verschillende niveaus en ontbreekt er een duidelijke wettelijke grondslag. Governance kan plaatsvinden op het niveau van een individuele organisatie, bijvoorbeeld binnen een bedrijf (*corporate governance*), maar als we het over bestuur hebben wordt meestal gedoeld op het bestuur van een staat. In deze context kan governance gedefinieerd worden als:

[6] SCADA staat voor Supervisory Control And Data Acquisition, PLC staat voor programmable logic controller.

[7] Schermer 2008.

[8] Hufty 2011, p. 405

[9] Art. 18 lid 2 Wegenverkeerswet.

"De uitoefening van economische, politieke en bestuurlijke macht. Het omvat de mechanismen, processen en instituties waardoor burgers hun belangen articuleren, hun rechten uitoefenen, hun plichten voldoen en hun disputen oplossen."[10]

Door de globalisering aan het begin van de 20e eeuw die uitmondde in de grote wereldoorlogen, groeide het besef van de noodzaak van governance op mondiaal niveau, zogenoemde *global governance*. Global governance houdt zich bezig met mondiale vraagstukken die niet binnen de context van een individuele natiestaat opgelost kunnen worden. Voorbeelden van deze vraagstukken zijn wereldvrede, internationale veiligheid, economische ontwikkeling en welvaartverdeling, milieuvraagstukken en – inmiddels ook – de regulering van het internet. Internet governance is zowel een onderdeel van als een katalysator voor global governance. Het internet roept enerzijds nieuwe mondiale vraagstukken op (denk bijvoorbeeld aan grensoverschrijdende cybercrime), anderzijds stimuleert het internet als wereldwijd communicatienetwerk het globaliseringsproces.

Door het toenemende economische en maatschappelijke belang van internet kwam het onderwerp internet governance eind jaren negentig steeds nadrukkelijker op de agenda van nationale staten en internationale organisaties, zoals de Verenigde Naties, te staan. Dit mondde uiteindelijk in 2003 en 2005 uit in de door de VN georganiseerde *World Summits on the Information Society* (WSIS). Tijdens de tweede internationale topconferentie werd ook een definitie van internet governance geformuleerd:[11]

"Internet governance is de ontwikkeling en toepassing door overheden, de private sector en het maatschappelijk middenveld van gedeelde principes, normen, besluitvormingsprocedures en programma's die de ontwikkeling en het gebruik van het internet vormgeven."

Achter deze brede definitie van internet governance gaan tal van perspectieven schuil. Kurbalija geeft een overzicht vanuit de achtergrond van betrokkenen met ieder hun eigen perspectief, zoals IT-specialisten die geïnteresseerd zijn in technische standaarden, communicatiewetenschappers die willen weten welke rol internet speelt bij communicatie, mensenrechtenspecialisten met interesse in de vrijheid van meningsuiting en privacy, andere juristen die vanuit het perspectief van jurisdictie en geschillenoplossing kijken, et cetera.[12] Los van de vraag of deze typeringen accuraat zijn, maakt het wel duidelijk dat de vragen die opkomen bij internet governance sterk gekleurd worden door het perspectief dat men heeft.

Enigszins in het verlengde van deze observatie ligt het onderscheid dat gemaakt wordt tussen technische en inhoudelijk vraagstukken op het gebied van internet governance. Technische aspecten vallen onder internet governance in *enge zin* en betreffen vraagstukken aangaande protocollen, standaarden, domeinnamen enzovoorts. Het gaat dan om de infrastructuur en het technisch ontwerp van internet. Internet governance in *brede zin* heeft betrekking op inhoudelijke, politieke of

---

[10] Definitie van de United Nations Development Programme, te vinden via: http://mirror.undp.org/magnet/policy/glossary.htm.

[11] Report of the Working Group on Internet Governance 2005, p. 4.

[12] Kurbalija, J. (2012), An Introduction to Internet Governance, DiploFoundation.

juridische vragen rondom specifieke thema's zoals auteursrecht, vrijheid van meningsuiting, privacy en e-commerce.

Dutton & Peltu hanteren een indeling waarin internet governance in brede en enge zin deels overlappen.[13] Internet governance in enge zin typeren zij als *internet centric*, het internet als zodanig staat daarbij centraal. Internet governance in brede zin delen zij op in *internet user centric* en *non-internet centric*. In de eerste categorie gaat het om regulering van gebruik en misbruik van het internet. Het draait hier om onderwerpen als cybercrime, consumentenbescherming en privacy.[14] De tweede categorie ziet op bredere maatschappelijke vraagstukken waarbij het internet weliswaar een belangrijke rol speelt, maar die niet exclusief het internet raken. Hierbij kan gedacht worden aan zaken als zoals het dichten van de digitale kloof, de toekomst van het auteursrecht, culturele diversiteit en de vrijheid van meningsuiting.

4 Het belang van internet governance

Al sinds de opkomst van het internet woedt er een discussie over de noodzaak, mogelijkheid en wenselijkheid van internet governance en regulering.[15] Vroege tegenstanders van internetregulering zagen het internet als een vrije wereld zonder regels. Zij waren van mening dat het internet een ongekende vrije uitwisseling van informatie op globale schaal zou moeten bewerkstelligen; internetregulering zou deze vrijheid van informatie onnodig beperken.[16] Voorstanders van regulering betwisten deze opvatting, zij beschouwen het internet als een ruimte voor menselijke interactie waar evengoed als in de fysieke wereld normen en waarden gelden die, waar noodzakelijk, door middel van wet- en regelgeving moeten worden afgedwongen.

Een vroeg internetreguleringsinitiatief is de door Al Gore geïnitieerde *High Performance Computing and Communication Act of 1991*. Deze wet richtte zich op het tot stand brengen van een goede en snelle informatie-infrastructuur en richtte zich daarmee dus op internet governance in enge zin. In 1998, toen in Nederland steeds meer bedrijven en huishoudens het internet dagelijks gebruikten, formuleerde de Nederlandse overheid voor het eerst een coherente visie op de toekomstige regulering van het internet. In de Nota Wetgeving voor de Elektronische Snelweg (WES) onderkende de overheid de sociale en economische veranderingen die de 'informatiesamenleving' teweeg zou brengen en het belang van regulering bij het in goede banen leiden van deze veranderingen.[17]

In de Nota WES werden drie situaties onderscheiden voor wat betreft het belang van internet binnen onze samenleving: 1) internet als luxegoed, 2) internet als infrastructuur naast bestaande infrastructuren (nevenschikking) en 3) internet als infrastructuur die andere infrastructuren vervangt

---

[13] Dutton, W.H. & Peltu, M. (2005), The Emerging Internet Governance Mosaic: Connecting the Pieces, http://ssrn.com/abstract=1295330.

[14] Voor meer over deze onderwerpen zie de hoofdstukken 5, 8, 9, 15 en 17 in dit boek [check drukproef]

[15] Segura-Serrano (2006), Internet Regulation and the Role of International Law, Max Planck Yearbook of United Nations Law, Volume 10, 2006, p. 193.

[16] Burton 1995.

[17] Kabinetsnota WES 1998, Tweede Kamer, vergaderjaar 1997-1998, 25 880, nrs. 1-2.

(verdringing).[18] Inmiddels hebben wij op veel gebieden het stadium van verdringing bereikt. Hierbij is het (nagenoeg) onmogelijk om als samenleving als geheel of individuele burger te functioneren zonder internet.

Kern bij het onderscheid tussen luxegoed, nevenschikking en verdringing is de idee dat naarmate het belang van het internet in de maatschappij toeneemt, ook het belang toeneemt om deze omgeving te reguleren. De mate van afhankelijkheid van burgers van elektronische diensten werd gezien als een leidende factor voor de rol van de overheid bij de regulering van het internet. Bij het niveau van luxegoed moest de overheid een terughoudende rol aannemen, terwijl bij het niveau van nevenschikking een meer ordenende rol van de overheid verwacht mocht worden. Indien er sprake is van verdringing van offline diensten door elektronische diensten en applicaties, is een pro-actieve houding van de overheid gepast.[19] Inmiddels is het internet uitgegroeid tot een kritieke infrastructuur voor onze maatschappij, net zoals gas, water en elektriciteit. Een kritieke infrastructuur kan worden gedefinieerd als:

"Een systeem, zowel fysiek als virtueel, dat zo vitaal is voor een land dat het wegvallen hiervan een verzwakkende invloed heeft op het sociaal en economisch functioneren en de nationale veiligheid."[20]

Dit gaat zeker op voor het internet, met name voor wat betreft het economisch functioneren van ons land. Daarnaast wordt het internet, zoals eerder gesignaleerd, steeds vaker gekoppeld aan fysieke infrastructuren. Waterschappen kunnen bijvoorbeeld hun pompen en afsluitsystemen via het internet aansturen.[21] Fouten binnen deze infrastructuur, of deze nu worden veroorzaakt door onzorgvuldig of crimineel menselijk handelen, of door soft- of hardware fouten, kunnen tot enorme schade leiden.

Omdat internet zo cruciaal is geworden voor onze economie, maatschappij en nationale veiligheid, staat de veiligheid van het internet (*cybersecurity*), hoog op de (inter)nationale agenda.[22] Hierbij draait het niet alleen om bescherming tegen cybercriminelen, hackers en technische kwetsbaarheden, maar ook om bescherming tegen door staten geïnitieerde cyberaanvallen. Zo is er in de Nederlandse Defensie Strategie nadrukkelijk aandacht voor oorlogsvoering via het internet (*cyberwarfare*) en voor *cyberspionage*.[23]

5 Vijf goverance modellen voor het internet

Het belang van het internet voor onze economie, maatschappij en nationale veiligheid noopt tot een effectieve reguleringsstrategie. Het traditionele governance model in de fysieke wereld is regulering

[18] Kabinetsnota WES 1998, p. 4

[19] Bovens 1999

[20] Kabinetsnota KWINT 2001, p.11

[21] Luijff 2004.

[22] Zie uitgebreider hoofdstuk 13 van dit boek.

[23] Zie Ministerie van Defensie (2012), Defensie Cyber Strategie.

van staatswege.[24] De staat stelt binnen de grenzen van het territoir de belangrijkste regels op en ziet toe op de handhaving daarvan. Dit traditionele, nationaal georiënteerde model van regulering is niet goed toepasbaar op transnationale vraagstukken, zoals internet governance.

Solum (2008) heeft een indeling gemaakt in vijf governance modellen voor het internet die, afhankelijk van het onderwerp, al dan niet in combinatie kunnen en moeten worden toegepast om tot een effectieve regulering van het internet te komen:

- Zelfregulering en spontane ordening;
- Nationale regulering van staatswege;
- Transnationale en internationale regulering;
- Regulering door technologie;
- Marktwerking.

Het eerste model gaat uit van zelfregulering door alle betrokken actoren en spontane ordening. Het is in de kern wat John Perry Barlow in zijn befaamde *Declaration of the Independence of Cyberspace* beschreef en wat Post (2009) op onderdelen verdedigt. De idee is dat de normering van het internet het beste aan de gebruikers zelf kan worden overgelaten en de overheid zich er buiten moet houden. De (idealistische) idee uit de *Declaration* was dat gebruikers zichzelf volgens de 'gouden regel' zouden organiseren. In bepaalde situaties is het model bruikbaar, maar in de praktijk blijkt dat te veel gebruikers zich bij het ontbreken van externe druk door handhavende instituties (privaatrechtelijk, bestuursrechtelijk, strafrechtelijk) onttrekken aan zelfregulering. Omdat bepaalde belangen vanwege hun maatschappelijke impact dusdanig zwaar wegen (denk aan mensenrechten of de bescherming van kritieke infrastructuren) dat handhaving noodzakelijk is, blijft een puur zelfregulerend model op het internet een utopie.

Het tweede model, dat ziet op regulering door nationale overheden, is dominant in de fysieke wereld, maar werd aanvankelijk als lastig of onmogelijk gezien voor het internet.[25] Binnen de grenzen van een land kan het internet echter wel degelijk effectief gereguleerd worden. Goldsmith & Wu betogen dan ook dat internetregulering primair nationaal georiënteerd is.[26] De nationale overheid kan regels stellen aan het gebruik van het internet door het reguleren van nationale netwerken en ISPs. In landen waar autoritaire regimes de vrijheid van meningsuiting beperken is dit duidelijk zichtbaar. In bijvoorbeeld China en Iran is de vrije toegang tot het internet beperkt. Door middel van filters, internetblokkades en toezicht op het gebruik van internet wordt nationale wetgeving gehandhaafd. Gebruikers proberen deze strategieën te ondermijnen door via beveiligde en anonieme verbindingen (VPNs, proxies, Tor) alsnog contact te maken met het grotere internet.

[24] Het betreft hier uiteraard een vergaande simplificatie van de werkelijkheid, waarin naast regulering van staatswege een complex geheel van formele en informele (zelf)reguleringsmechanismen de maatschappij ordent.

[25] Zie voor de redenen hiervoor paragraaf 6.

[26] Goldsmith, J. & T. Wu (2008). Who Controls the Internet? Illusions of a Borderless World. Oxford University Press.

Het derde model omvat twee afzonderlijke modellen die regulering door de nationale staat overstijgen. In de eerste plaats valt er internationale regulering door verdragen onder. Een voorbeeld is het Cybercrime-verdrag (zie hoofdstuk 9). In de tweede plaats wordt er regulering door transnationale organisaties, dat wil zeggen non-gouvermentele, internationale organisaties die op grond van overeenstemming tussen betrokken partijen (delen van) het internet reguleren, onder begrepen. ICANN is daarvan het meest succesvolle voorbeeld. Het betreft hier evenwel over het algemeen enkel internet governance in enge zin (afspraken over de technische werking van het internet).

Het vierde model sluit aan bij Lessig's concept van *Code as Law*.[27] Normering kan besloten liggen in de vormgeving van de technische toepassingen en de architectuur van het internet. Zo kan normconform of gewenst gedrag worden afgedwongen door de mogelijkheden (en onmogelijkheden) die de technologie de gebruiker biedt.[28] Hierbij kan gedacht worden aan filters waardoor een gebruiker bepaalde websites niet kan bezoeken, maar ook aan de vorm van een webpagina die bepaalt hoe een gebruiker moet navigeren en welke content hij kan zien.

Het vijfde en laatste model is gebaseerd op marktwerking en laat zien dat gezichtsbepalende spelers van het internet, zoals Google, Yahoo en Amazon, door hun grote macht tot op zekere hoogte zelf de normen bepalen. De marktwerking reguleert echter ook het gedrag van deze bedrijven. Wanneer diensten niet langer aantrekkelijk zijn voor gebruikers, bijvoorbeeld omdat de bedrijven onzorgvuldig omgaan met de privacy van gebruikers, dan zullen deze gebruikers overstappen naar alternatieve diensten.

6 Complicerende factoren bij internet governance en regulering

Hoewel er ontegenzeggelijk een belang is om het internet te reguleren, kent het internet een aantal specifieke eigenschappen die effectieve regulering compliceren. Hieronder worden de belangrijkste complicerende factoren genoemd en toegelicht. Het betreft hier met name complicaties voor de traditionele regulering van staatswege (nationaal en internationaal).

6.1 Geen beperkingen in ruimte

Het internet kent geen beperkingen in ruimte en eindigt niet bij de landsgrens, waardoor iedere regulerende strategie problemen zal ondervinden met betrekking tot het uitoefenen van rechtsmacht.[29] Daar waar grenzen in de fysieke wereld grotendeels rechtsmacht bepalen, vervallen deze in de online wereld.[30] Rechtsmacht kent verschillende dimensies, met betrekking tot het internet zijn met name prescriptieve jurisdictie en handhavingsjurisdictie relevant.[31]

---

[27] Lessig 2006.

[28] Een anologie uit de fysieke wereld is de snelheidsdrempel: door de snelheidsdrempel wordt normconform gedrag afgedwongen, ook al is er niet noodzakelijkerwijs 'respect voor de regel'.

[29] Lessig, L. (2006), Code Version 2.0, New York: Basic Books.

[30] Johnson, D.R. & D.G. Post (1996), Law And Borders: The Rise of Law in Cyberspace, 48 Stanford Law Review 1367.

[31] Wij beschouwen hier handhaving vanuit het perspectief van de staat. Verhoudingen tussen individuele partijen kunnen bijvoorbeeld via het internationaal privaatrecht (effectief) worden gereguleerd. Naast prescriptieve jurisdictie en handhavingsjurisdictie kunnen we ook nog

Prescriptieve jurisdictie

Prescriptieve of wetgevende jurisdictie betreft de vraag of een staat rechtsmacht kan aannemen met betrekking tot bepaalde gedragingen. Aanknopingspunten voor het aannemen van rechtsmacht door een staat zijn territorialiteit, het gevolg van de gedraging, de nationaliteit van het rechtssubject, universaliteit en de bescherming van de belangen van de staat.[32]

Maar een probleem dat zich op het internet manifesteert, is dat met name het belangrijkste aanknopingspunt voor het aannemen van rechtsmacht (territorialiteit) niet meer af te bakenen valt. Dit leidt tot het probleem van 'botsende soevereiniteit'.[33] Dit probleem treedt op wanneer staten verschillend denken over de strafbaarheid van gedragingen en de noodzaak om bepaald gedrag te reguleren. Zo kunnen gegevens (zoals pornografisch materiaal of een politieke uiting) in het ene land binnen de grenzen van de vrijheid van meningsuiting vallen, maar strafbaar zijn in een ander land. Het internet zorgt er voor dat burgers van het land waar de uiting strafbaar is toch toegang kunnen krijgen tot de gegevens die legaal in het andere land worden aangeboden.

Handhavingsjurisdictie

Handhavingsjurisdictie betreft de vraag in hoeverre een staat (dwang)middelen en (opsporings)bevoegdheden mag inzetten tegen burgers en is daarmee nauw verbonden met de nationale soevereiniteit. Handhavingsjurisdictie is in principe beperkt tot de eigen landgrenzen. Wil een staat dwangmiddelen of opsporingsbevoegdheden inzetten tegen burgers die zich buiten het eigen territoir bevinden, dan moet hiervoor via een rechtshulverzoek toestemming worden gevraagd aan het land waar de middelen ingezet moeten worden. Verzoeken tot wederzijdse rechtshulp zijn echter vaak duur en tijdsintensief, waardoor internationale onderzoeken belemmerd worden. Dit is des te problematischer op het internet waar gedragingen door het ontbreken van fysieke beperkingen vaak plaatsvinden in meerdere jurisdicties. Zo kan een crimineel in India via een server in Brazilië een computer in Duitsland hacken om vervolgens daarmee een Nederlandse gebruiker aan te vallen. Problematisch voor opsporingsautoriteiten in het digitale tijdperk is verder dat zij niet altijd meteen kunnen achterhalen waar op de wereld een verdachte zich bevindt en/of waar bepaalde (strafbare) gegevens zijn vastgelegd en opgeslagen. Wanneer gewacht moet worden op internationale rechtshulp kan het zijn dat de crimineel reeds zijn sporen heeft gewist.[34]

6.2 Anonimiteit

Communicatie en contact op internet vindt over (grote) afstanden plaats. Omdat de communicatie tussen personen indirect is, zal deze communicatie vaak anoniem zijn. Anonimiteit helpt gebruikers zich te uiten en om hun identiteit en interesses te ontdekken zonder dat dit gedrag door bijvoorbeeld overheden onder de loep wordt genomen. Er schuilen echter ook gevaren in anonimiteit. Burgers,

---

adjudicatieve jurisdictie onderscheiden (welke rechter is bevoegd). Adjudicatieve jurisdictie valt echter vaak samen met prescriptieve jurisdictie.

[32] Koops, B.J. & Lips, A.M.B. (2003). Wie reguleert het internet? Horizontalisering en rechtsmacht bij de technische regulering van het internet. Verschenen in: *Zeven essays over informatietechnologie en recht*. (pp. 261-315). Den-Haag: Sdu uitgevers, p. 301.

[33] Lessig, L. (2006), Code Version 2.0, New York: Basic Books, p. 281.

[34] Minister van Justitie en Veiligheid I.W. Opstelten, Brief aan de Tweede Kamer inzake Wetgeving bestrijding cybercrime, 15 oktober 2012.

consumenten, bedrijven en overheden kunnen makkelijker het slachtoffer worden van grove belediging, uitbuiting en crimineel gedrag, zonder dat de dader hiervan kan worden achterhaald. Het is daarom van belang dat er een goede balans wordt getroffen tussen anonimiteit en aansprakelijkheid.[35] Zonder daadwerkelijk aansprakelijkheid te kunnen worden gesteld of de angst voor consequenties zijn mensen sneller geneigd onwenselijk gedrag door te zetten.[36]

Anonimiteit levert vanuit het oogpunt van internet governance en internetregulering met name een attributieprobleem op: wie is verantwoordelijk voor een bepaalde gedraging online en welk (juridisch) instrumentarium kan een staat inzetten als reactie op deze gedraging? Deze vraag speelt in het bijzonder in de context van cybercrime en cyberwarfare. Het juridisch instrumentarium in het geval van cybercrime is het strafrecht, het instrumentarium bij cyberwarfare is het oorlogsrecht. Het probleem is evenwel dat door anonimiteit veelal niet duidelijk is of de dader een individuele crimineel is, of een actor die in dienst van een staat handelt.[37]

6.3 Technologische turbulentie

Een van de moeilijkheden bij het reguleren van gedrag op het internet is dat het internet en daaraan gerelateerde technologieën zich razendsnel ontwikkelen. Het opstellen van wetgeving daarentegen is een tijdsintensief proces. Hierdoor loopt nieuwe regelgeving welhaast per definitie altijd een stap achter op de technologische werkelijkheid. Om hier aan tegemoet te komen, kunnen wetten open en technologie-neutraal worden geformuleerd. Een probleem hierbij is echter dat de wet door zijn open normen en formuleringen vaag en dubbelzinnig kan zijn, waardoor het onduidelijk is wanneer of op wie een bepaling van toepassing is. Hierdoor ontstaat mogelijk rechtsonzekerheid.

6.4 Complexiteit

Het internet kenmerkt zich door een hoge mate van technische en organisatorische complexiteit. Hierdoor is het niet eenvoudig om effectieve reguleringsstrategieën te formuleren en uit te voeren. Zoals aangegeven in het begin van dit hoofdstuk is het alleen mogelijk om effectieve wet- en regelgeving voor het internet op te stellen met een gedegen kennis van de werking van het internet. De wetgever beschikt niet altijd over deze kennis. Daarnaast is de wetgever, bijvoorbeeld bij cybercrime, niet altijd bekend met de aard van het probleem, de omvang en de schade.

7 Wie is verantwoordelijk voor internet governance?

Een complex geheel van actoren en belanghebbenden is betrokken bij internet governance. Hoewel de regulering van het internet in belangrijke mate wordt vormgegeven door staten, op basis van nationale wetgeving en internationale verdragen, hebben we uit de vorige paragrafen op kunnen maken dat de effectiviteit van dit model beperkingen kent. Ook de overige governance modellen die wij besproken hebben moeten daarom in ogenschouw worden genomen.

---

[35] Schermer & Wagemans 2010, p. 39.

[36] Zie bijvoorbeeld Solove 2007, p. 146. Hierin wordt als voorbeeld gegeven dat we eerder geneigd zijn om iemands privacy aan te tasten of valsheden te verspreiden via internet als we anoniem blijven, door gebrek aan consequenties en aansprakelijkheid. Hij noemt dit “the law of anonymity”.

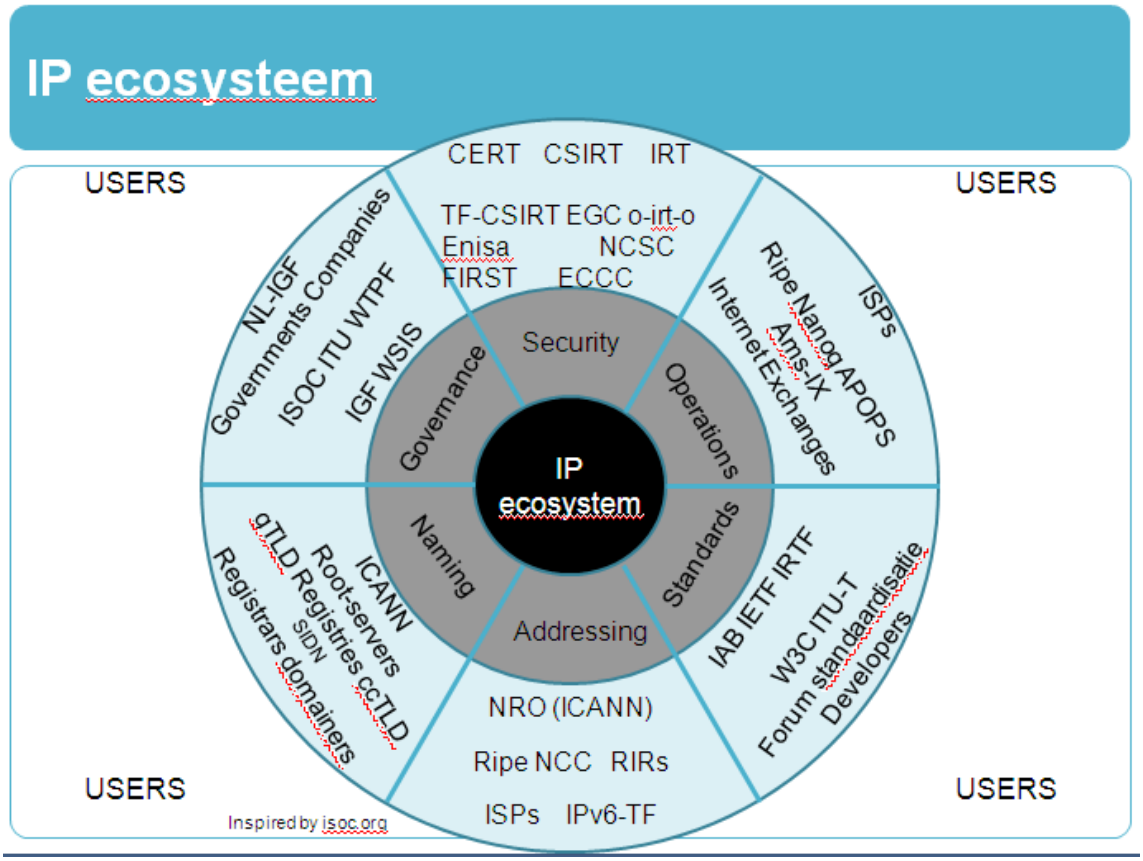
[37] Boer, L.J.M. & A.R. Lodder (2012), Chapter 10 Cyberwar (Cyberwar: What Law to Apply? And to Whom?), in: Leukfeldt/Stol (eds.), Cyber Safety: An Introduction, Eleven Publishing, zie ook http://ssrn.com/id=2039220.

Er is een belangrijke stroming van experts en politici die benadrukken dat er gewerkt moet worden aan regulering van nieuwe technologie op basis van afspraken tussen publieke, private en maatschappelijke partijen. Dit laatste model wordt *multi-stakeholder governance* genoemd. Binnen dit multi-stakeholder-model kunnen ook verschillende modellen van internet governance worden betrokken.

Het multi-stakeholder-denken vindt haar oorsprong in het feit dat de technische infrastructuur van het internet veelal in handen is van private partijen, waarmee de feitelijke beschikkingsmacht niet exclusief bij nationale staten ligt. Ook zal technologische ontwikkeling voornamelijk vanuit de private sector komen, waardoor het zinvol is om regelgeving samen met de sector vorm te geven. Daarnaast speelt in het multi-stakeholder-denken ook mee dat wanneer de controle over het internet volledig bij staten wordt gelegd, dit mogelijk een gevaar oplevert voor mensenrechten, zoals de vrijheid van meningsuiting, de vrijheid van nieuwsgaring en het recht op privacy. Een veelgehoord argument voor multi-stakeholder-denken is tenslotte dat volledige staatscontrole over het internet mogelijk nadelige gevolgen heeft voor vrije mededinging en innovatie. De meeste Westerse landen zijn om deze redenen aanhanger van het multi-stakeholder-model voor internet governance.

In deze paragraaf bespreken wij een aantal belangrijke *stakeholders* op het gebied van internet governance die binnen het multi-stakeholder model actief zijn. Wij richten ons hierbij specifiek op die organisaties, fora en gremia die specifiek zijn voor het internet. Uiteraard spelen in de bredere discussie over global governance en internet governance (inter)gouvernementele organisaties en non-gouvernementele organisaties, zoals de Verenigde Naties, de Europese Unie, de OESO, de WTO, Oxfam, Amnesty International en Free Press Unlimited een rol, maar deze zullen wij in dit kader niet nader bespreken.

Onderstaande afbeelding van Erik Huizer geeft een goed overzicht van de verschillende actoren die betrokken zijn bij de regulering van het IP-ecosysteem en daarmee het internet (in enge zin en deels ook in brede zin).



Internet Corporation for Assigned Names and Numbers (ICANN)

De Internet Corporation for Assigned Names and Numbers (ICANN) coördineert de belangrijkste technische processen die het internetverkeer mogelijk maken. Deze processen zijn het domeinnaamsysteem (DNS) en het stelsel van Internet Protocol (IP) adressen. ICANN is een private organisatie. De hierboven genoemde sleutelfuncties voor het dagelijks beheer worden uitgeoefend door de Internet Assigned Numbers Authority (IANA) dat een onderdeel van ICANN is. ICANN vervult haar functies in opdracht van de Amerikaanse overheid op basis van een specifiek contract.

ICANN heeft naast haar beheerrol ook een strategische rol op het gebied van het ontwikkelen van beleid, technische standaarden en IT protocollen. Beleidsmatige aspecten van internetregulering die vorm hebben gekregen onder het gezag van ICANN zijn: het bevorderen van concurrentie in de markt voor uitgifte en beheer van domeinnamen, het opzetten van uniforme geschillenbeslechting met betrekking tot domeinnamen (*Uniform Domain Name Dispute Resolution Policy*, UDRP) en het ontwikkelen van veiligheidsmaatregelen tegen cybercrime.[38]

De organisatie is opgebouwd uit een centraal bestuur met daaronder diverse werkgroepen, adviescomités en ondersteunende organisaties, die elk een eigen technisch deelgebied voor hun rekening nemen. De eenheden werken samen volgens een interne code: de ICANN By-laws. Bij het formuleren van strategisch beleid staat ICANN zoveel mogelijk open voor ideeën vanuit de private sector en relevante spelers in de internetwereld. Deelname aan ICANN-congressen en werkgroepen

[38] Domain Name System Security Extensions (DNSSEC).

is in principe vrij toegankelijk voor een ieder die daaraan wil bijdragen. ICANN streeft ernaar te handelen op basis van een zo groot mogelijke consensus en heeft daarom een breed netwerk van registries, registrars, Internet Service Providers (ISPs), overheden en experts op het gebied van intellectuele eigendom, mensenrechten en online handel opgebouwd.

Gezien het immense belang van de coördinerende taken van ICANN voor het functioneren van het internet is het werk van de organisatie sterk gepolitiseerd. Het is een publiek geheim dat de Amerikaanse overheid nog steeds een grote invloed uitoefent op het dagelijks bestuur van ICANN. Via de *Government Advisory Comittee* (GAC) brengen bovendien ook de overheden van andere landen hun zienswijzen op het beleid van ICANN onder de aandacht van het ICANN bestuur. De adviezen van GAC zijn echter niet bindend voor de organisatie, hetgeen enerzijds uiting geeft aan de multi-stakeholder-gedachte, maar anderzijds reden is voor politieke spanning tussen ICANN, de VS en de overige deelnemende landen.

Internet Engineering Task Force (IETF)

De *Internet Engineering Task Force* (IETF) is een groot, internationaal samenwerkingsverband dat zich bezighoudt met het ontwikkelen van technische standaarden en beleid voor het internet.[39] Deelname aan de IETF staat open voor iedere geïnteresseerde persoon. De IETF wordt gefaciliteerd door de non-profit organisatie *Internet Society* (ISOC).[40]

De officiële documenten die de IETF produceert worden *Requests for comments* (RFCs) genoemd. Hierin wordt beschreven hoe protocollen, standaarden en producten op het internet beter geïmplementeerd kunnen worden en hoe de internetgemeenschap technische vooruitgang kan boeken. Sommige van deze documenten worden als standaarden gezien. Documenten en zienswijzen van de IETF hebben op zichzelf geen juridische betekenis, maar zijn in de (technische) wereld wel gezaghebbend. De IETF heeft daardoor een grote invloed op de ontwikkeling en regulering van technische aspecten van het wereldwijde internet.

Een belangrijk onderdeel van de IETF is de *Internet Architecture Board* (IAB). De IAB is het onderdeel van de IETF dat de werkzaamheden van de IETF aanstuurt.

ITU

Met de komst van telegraaflijnen in de 19e eeuw werd het al snel duidelijk dat het noodzakelijk was om internationale afspraken te maken over zowel de aanleg als het gebruik van telecommunicatieverbindingen. In 1865 is daarom de *International Telegraph Union* opgericht in Parijs. Sinds 1934 heet de organisatie de *International Telecommunications Union* (ITU) en in 1947 werd ITU een agentschap van de Verenigde Naties. ITU is een intergouvernementele organisatie, waarbinnen zo'n 193 landen vertegenwoordigd zijn, maar de ITU is vanaf het begin gericht op samenwerking tussen beleidsmakers en de private (telecom)sector. Tegenwoordig zijn er meer dan 500 private ITU-leden.[41]

---

[39] De IETF heeft ook een 'zusterorganisatie' die zich specifiek bezighoudt met onderzoek en ontwikkeling van de technische standaarden voor het internet: de Internet Research Task Force (IRTF).

[40] Zie www.internetsociety.org/internet/what-internet/history-internet/ietf-and-internet-society.

[41] Zie http://www.itu.int/online/mm/scripts/mm.list?_search=ITUstates&_languageid=1.

De afspraken in ITU-verband zijn internationale overeenkomsten en verdragen. Deze afspraken zijn slechts bindend voor de stakeholders die hiermee instemmen en staten die de verdragen daadwerkelijk ratificeren. De besluitvorming is echter van oudsher sterk op consensus gericht zodat er door de jaren heen een stelsel van verdragen en standaardisatiebepalingen over de telecomsector is ontstaan in ITU-verband dat in feite een wereldwijd regelgevend kader vormt.

De organisatie houdt zich bezig met regulering en internationale standaardisatie op het gebied van IT en telecommunicatie. De ITU is momenteel verdeeld in drie eenheden die zich toeleggen op de drie belangrijkste werkterreinen van ITU. Dit zijn telecom (ITU-T), radiocommunicatie (ITU-R) en duurzame ontwikkeling (ITU-D).

Met de opkomst van internet en moderne ICT is de invloed van ITU langzamerhand gegroeid. Hoewel ITU formeel niet over het internet gaat, zijn vele aspecten van telecommunicatie en IT die door de ITU worden besproken randvoorwaardelijk voor de ontwikkeling van het internet. Begin 20e eeuw was het vanzelfsprekend dat overheden in internationaal verband afspraken maakten en verdragen sloten over telegraaflijnen en het opkomende telefoonverkeer. Anno 2013 is er echter sterke politieke verdeeldheid over de vraag of het reguleren van internet en technologie nog wel een taak is van primair overheden. Een aantal landen en non-gouvernementele organisaties op het gebied van mensenrechten vrezen dat een te grote controle op het internet door (autoritaire) staten negatieve gevolgen heeft voor mensenrechten als de vrijheid van informatie, vrijheid van meningsuiting en vrijheid van nieuwsgaring.

Deze discussie leidde in december 2012 tot een politieke confrontatie toen een aantal landen, onder leiding van Rusland, een voorstel indienden tot wijziging van de *International Telecommunications Regulations* (ITRs), waardoor de ITU expliciete bevoegdheden op het gebied van internetregulering zou krijgen. Het nieuwe verdrag is door slechts 89 landen ondertekend en daarmee niet bindend voor die landen die niet ondertekend hebben.[42] Met name Westerse landen, die een expliciete regulerende bevoegdheid van de VN-organisatie ten aanzien van het internet onwenselijk vinden, wijzen deze ontwikkeling af en zijn dus niet gebonden door de nieuwe ITRs.

WSIS en IGF

De Algemene Vergadering van de VN riep in een resolutie uit 2001 op tot het beleggen van een conferentie over de informatiemaatschappij.[43] Dit werd de eerder genoemde World Summit on the Information Society (WSIS) en was een van de eerste gezaghebbende mondiale politieke conferenties waar is gesproken over internetregulering en de rol van overheden en internationale organisaties daarin.[44]

De International Telecommunication Union (ITU) nam het voortouw met de organisatie van WSIS en koos er voor om naast overheidsdelegaties ook internationale organisaties, bedrijven en

[42] http://www.itu.int/osg/wcit-12/highlights/signatories.html

[43] UN General Assembly Resolution 56/183 (21 December 2001)

[44] Er is twee maal een WSIS-top gehouden. De eerste was in Geneve van 10 tot 12 december 2003 en de tweede werd gehouden in Tunis, van 16 tot 18 november 2005.

maatschappelijke belangenorganisaties bij het proces te betrekken.

Er zijn twee WSIS-bijeenkomsten geweest. Het eerste deel van WSIS werd afgesloten met de Geneva *Declaration of principles* en het *Geneva Plan of Action*.[45] De tweede WSIS conferentie in 2005 resulteerde in de Tunis Agenda voor de Informatiemaatschappij, waarin het fundament gelegd is voor het debat over de regulering van het internet. Deze basis bestond uit de volgende politieke besluiten:

- Het vaststellen van de uitgangspunten van het VN ICT-beleid in de *WSIS Action Lines*.[46] Tijdens de WSIS is bepaald dat de implementatie van de ideeën van de WSIS op nationaal niveau via 'Action Lines' moet gaan. Deze Action Lines zien onder andere op de rol die de overheid en andere actoren kunnen spelen in de toepassing van ICT voor ontwikkelingsdoeleinden;
- De oprichting van het *Internet Governance Forum* (IGF). Het forum is een internationaal platform voor beleidsoverleg met een multidisciplinair karakter, net als de WSIS conferenties. IGF heeft slechts een adviserende rol binnen de VN-besluitvorming. Hoewel besluiten en standpunten van het IGF geen formele juridische status hebben, zijn zij niettemin relevant vanwege het feit dat het gezaghebbende uitspraken over internetregulering betreft vanuit het bedrijfsleven, maatschappelijke organisaties en andere non-gouvernementele organisaties, die tot stand komen in samenspraak met overheden. Daarnaast speelt IGF een belangrijke agendavormende rol in het politieke proces rondom internetregulering. In het IGF komen bedrijven en organisaties bijeen om met overheidsvertegenwoordigers van gedachten te wisselen over internetregulering;
- Het aanwijzen van ICANN als wereldwijde autoriteit op het gebied van DNS management. De facto werd ICANN daarmee het eerste orgaan met enig regulerend gezag over het internet dat als zodanig internationaal erkend is;
- De oprichting van een multidisciplinaire conventie van belanghebbenden op het gebied van internetregulering en experts op het gebied van de universele mensenrechten. Deze werkgroep kreeg als taak om documenten op te stellen waarin de rechten van de mens op internet werden vastgesteld, een specifieke toepassing van de universele verklaring van de rechten van de mens op het digitale domein. Tijdens de WSIS conferentie werd vastgesteld dat de vrijheid van meningsuiting, het recht op privacy en het recht op vrije vereniging de belangrijkste 'online' mensenrechten zijn. Daaraan werd specifiek toegevoegd het universele recht op betaalbare toegang tot het internet.

In de Tunis Agenda voor de informatiemaatschappij is opgenomen dat de WSIS Actielijnen en het Geneva Plan of Action gefaciliteerd moeten worden door de VN en dat met name ITU, UNESCO en UNDP een leidende rol in dit proces moeten krijgen. Mede op basis van deze declaratie is een groot aantal VN organisaties initiatieven gaan ontplooien die het terrein van internetregulering raken en die het ICT-beleid van nationale overheden beïnvloeden. Deze organisaties belichten het ICT-beleid echter elk vanuit hun eigen deelbelang. Zo ziet UNESCO graag dat de cultuurgoederen van de wereld worden bewaard en beschikbaar gesteld via het internet, terwijl UNDP de ontwikkeling van internet

[45] Zie https://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160.
[46] Zie http://www.itu.int/wsis/stocktaking/help-action-lines.html.

en ICT ziet als een belangrijk middel om de *Millennium Development Goals* van de VN te halen. Daarmee is het voor beleidsmakers en juristen dikwijls lastig om de politieke idealen om te zetten naar een praktisch toepasbaar juridisch kader voor de online wereld.

Na de WSIS conferenties is de beweging voortgezet in het zogenaamde *WSIS Stocktaking Proces*. Dit proces, gebaseerd op een resolutie van de ECOSOC, is bedoeld om de voortgang van de WSIS actielijnen te bewaken en is een belangrijke bron van academische kennisvorming en publicaties op het gebied van ICT-regulering. Nog altijd zijn de WSIS Action Lines hiervoor de leidraad.[47] Tevens wordt er jaarlijks een bijeenkomst van het Internet Governance Forum gehouden.[48]

8 Afsluitende bespiegeling

Sommigen voorspellen de ondergang van het internet. Hoewel de toepassingen kunnen wijzigen en de grip van de overheid kan toe- of afnemen, zal de mensheid zich niet snel de verworvenheid van het wereldwijd kunnen communiceren laten afnemen. Om die reden verwachten wij dat internet governance en -regulering ook in de toekomst van groot belang zal blijven.

[47] ECOSOC Resolution 2010/2 on "Assessment of the progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society". Zie voor meer informatie: WSIS Stocktaking Report.

[48] www.intgovforum.org

Gebruikte en aanbevolen literatuur

Boer, L.J.M. & A.R. Lodder (2012), Chapter 10 Cyberwar (Cyberwar: What Law to Apply? And to Whom?), in: Leukfeldt/Stol (eds.), Cyber Safety: An Introduction, Eleven Publishing, zie ook http://ssrn.com/id=2039220

Bovens, M.A.P. (1999) *Overheidsinterventie in de informatiemaatschappij*, Universiteit Utrecht (oratie).

Burton (1995), Regulation and control of the Internet: is it feasible? Is it necessary?, in: *Journal of Information Science*, december 1995 vol. 21 no. 6, pp. 413-428.

Bygrave, L. A., & Bing, J. (red.) (2009), *Internet Governance: Infrastructure and Institutions*. Oxford: Oxford University Press

Dutton, W.H. & Peltu, M. (2005), *The Emerging Internet Governance Mosaic: Connecting the Pieces*, (via: http://ssrn.com/abstract=1295330)

Dutton, W.H. (2013) *The Oxford Handbook of Internet Studies*, Oxford: Oxford University Press.

Goldsmith, J. (2000), Unilateral Regulation of the Internet: A Modest Defence, in: *European Internet Law Journal*, Vol. 11 no 1, p. 135-148.

Goldsmith, J. & T. Wu (2008). *Who Controls the Internet? Illusions of a Borderless World*, Oxford: Oxford University Press

Hufty, M. (2011). Investigating Policy Processes: The Governance Analytical Framework (GAF), in: *Research for Sustainable Development: Foundations, Experiences and Perspectives*, red. Wiesmann, U, Humi H., Geographica Bernensia, 2011, p. 403-424

Johnson, D.R. & D.G. Post (1996), Law And Borders: The Rise of Law in Cyberspace, in: Stanford Law Review, 48, 1367

Koops, B.J. & Lips, A.M.B. (2003). Wie reguleert het internet? Horizontalisering en rechtsmacht bij de technische regulering van het internet. Verschenen in: *Zeven essays over informatietechnologie en recht*. (pp. 261-315). Den-Haag: Sdu uitgevers

Kulesza, J. (2012). *International Internet Law*, New York: Routledge

Kurbalija, J. (2012), *An Introduction to Internet Governance*, DiploFoundation

Lessig, L. (2006), Code version 2.0, New York: Basic Books

Lodder, A.R. e.a. (2010). *Recht en web 2.0*, NVvIR publicatiereeks, nummer 27, Amsterdam: Lulu

Lodder, A.R. & Vaisnoriene, N. (2010). Internet governance en regulering: boeiende analyses, nuttige handreikingen maar nog veel open vragen. Tijdschrift voor Internetrecht, 3(5), 153-157

Lodder, A.R. (2012). Recht rond cyberwar, internet van dingen en andere internet (on)gemakken: de tien geboden van het internetrecht. (2012, maart 30). Amsterdam: Lulu.

Luijff, H.A.M. (2004) De kwetsbaarheid van de ICT-Samenleving, Justitiële verkenningen, jaargang 30, nummer 8, 2004, p. 22- 33

Marsden, C.T. (2011), Internet Co-Regulation. Cambridge University Press

Mueller, M. (2010), Networks and States: The Global Politics of Internet Governance. MIT Press

Post, D.G. (2009), In Search of Jefferson's Moose: Notes on the State of Cyberspace. Oxford University Press

Savin, A. (2013), EU Internet Law, Edward Elgar Pub.

Schermer, B.W. (2008), Ambient Intelligence, persoonsgegevens en consumentenbescherming, Leidschendam: ECP.NL

Schermer, B.W. & T. Wagemans (2010), Freedom in the Days of the Internet. CES 2010

Segura-Serrano, A. (2006), Internet Regulation and the Role of International Law, Max Planck Yearbook of United Nations Law, Volume 10, 2006, p. 193

Solove, D.J. (2007), The future of Reputation, Yale University Press, 2007

Solum, L.B. (2008), Models of Internet Governance, Illinois Public Law Research Paper No. 07-25, http://ssrn.com/abstract=1136825

Zittrain, J. (2008) The Future of the Internet and How to Stop It. Yale University Press